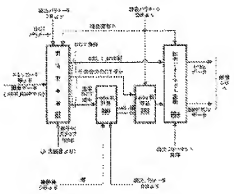
DEVICE AND METHOD FOR PROCESSING IMAGE

Publication number: JP2001203878 (A)
Publication date: 2001-07-27
Inventor(s): KAMIJO KOICHI; MORIMOTO NORISHIGE; TONEGAWA SATOKO
Applicant(s): IBM
Classification:
- international: ***H04N5/91; G06T1/00; G06T9/00; H04N1/387; H04N1/40; H04N1/41; H04N7/30;*** **H04N5/91; G06T1/00; G06T9/00; H04N1/387; H04N1/40; H04N1/41; H04N7/30;** (IPC1-7): H04N1/387; G06T1/00; H04N1/40; H04N1/41; H04N5/91; H04N7/30
- European: G06T1/00W8C; G06T9/007
Application number: JP20000012520 20000121
Priority number(s): JP20000012520 20000121

Also published as:
JP3683766 (B2)
US2001010729 (A1)
US7046817 (B2)
GB2359211 (A)
GB2359211 (B)

Abstract of **JP 2001203878 (A)**

PROBLEM TO BE SOLVED: To prevent embedded authentication information from being lost, even if quantizing processing is performed after the authentication information is embedded.
SOLUTION: A pre-embedding part 32 converts the value of image data, so that the value after quantizing processing can not be changed by an error added by embedding processing of embedded data. A hash value calculating part 300 calculates a hash value from image data and key information and a hash value embedding part 302 embeds the hash value in the image data. An output format converting part 304 generates JPEG data, by applying quantizing processing or the like to the image data embedded with the hash value.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－203878
（P2001－203878Ａ）
(43)公開日　平成13年７月27日(2001.7.27)

(51)Int.Cl.⁷	識別記号	ＦＩ			ﾃｰﾏｺｰﾄﾞ（参考）
Ｈ０４Ｎ	1/387	Ｈ０４Ｎ	1/387		５Ｂ０５７
Ｇ０６Ｔ	1/00		1/41	Ｂ	５Ｃ０５３
Ｈ０４Ｎ	1/40	Ｇ０６Ｆ	15/66	Ｂ	５Ｃ０５９
	1/41	Ｈ０４Ｎ	1/40	Ｚ	５Ｃ０７６
	5/91		5/91	Ｐ	５Ｃ０７７

審査請求　有　請求項の数15　ＯＬ　（全 25 頁）　最終頁に続く

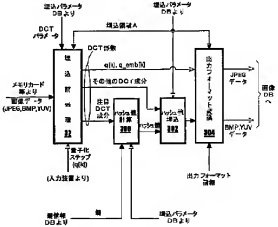
(21)出願番号　特願2000－12520(Ｐ2000－12520)
(22)出願日　平成12年１月21日(2000.1.21)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(74)代理人　100086243
弁理士　坂口　博　（外１名）

最終頁に続く

(54)【発明の名称】　画像処理装置およびその方法

(57)【要約】
【課題】　認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがないようにする。
【解決手段】　埋込前処理部３２は、埋め込みデータの埋め込み処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する。ハッシュ値計算部３００は、画像データと鍵情報からハッシュ値を計算し、ハッシュ値埋込部３０２は、画像データにハッシュ値を埋め込む。出力フォーマット変換部３０４は、ハッシュ値が埋め込まれた画像データを量子化処理などし、ＪＰＥＧデータを生成する。



【特許請求の範囲】
【請求項１】所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換手段（３２）と、
画像データに対して前記所定の処理を行う処理手段（３００，３０２）と、
前記所定の処理がなされた画像データを量子化処理する量子化手段（３０４）とを有する画像処理装置。
【請求項２】前記処理手段は、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い（５０）、
前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出手段（６０）をさらに有する請求項１に記載の画像処理装置。
【請求項３】前記変換手段は、
画像データに含まれる画素それぞれの形式を変換する形式変換手段（３２６，３３０）と、
前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節手段（３３２）とを有し、
前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す請求項１に記載の画像処理装置。
【請求項４】前記処理手段は、前記画像データに対して埋込データを埋め込む埋込処理を前記所定の処理として行う請求項１に記載の画像処理装置。
【請求項５】前記処理手段は、所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算手段（３００）と、
計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理手段（３０２）とを有する請求項４に記載の画像処理装置。
【請求項６】前記画像データに埋め込まれた埋込データを検出する検出手段（３０）をさらに有する請求項４または５に記載の画像処理装置。
【請求項７】前記量子化された画像データを逆量子化する逆量子化手段（４２２）と、
前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出手段（４００）と、
前記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算手段（４０２）と、
前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出手段（４０４）とを有する請求項５に記載の画像処理装置。
【請求項８】所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換し、
画像データに対して前記所定の処理を行い、
前記所定の処理がなされた画像データを量子化処理する画像処理方法。
【請求項９】所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換ステップと、
画像データに対して前記所定の処理を行う処理ステップと、
前記所定の処理がなされた画像データを量子化処理する量子化ステップとをコンピュータに実行させるプログラムを記録した記録媒体。
【請求項１０】前記処理ステップは、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い、
前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出ステップをさらに有する請求項９に記載の記録媒体。
【請求項１１】前記変換ステップは、
画像データに含まれる画素それぞれの形式を変換する形式変換ステップと、
前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節ステップとを有し、
前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す請求項９に記載の記録媒体。
【請求項１２】前記処理ステップは、前記画像データに対して埋込データを埋め込む埋込処理を前記所定の処理として行う請求項９に記載の記録媒体。
【請求項１３】前記処理ステップは、
所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算ステップと、
計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理ステップとを有する請求項１２に記載の記録媒体。
【請求項１４】前記画像データに埋め込まれた埋込データを検出する検出ステップをさらに有する請求項１２または１３に記載の記録媒体。
【請求項１５】前記量子化された画像データを逆量子化する逆量子化ステップと、
前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出ステップと、
前記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算ステップと、
前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出ステップとを有する請求項１３に記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、著作権情報などの認証情報（埋め込みデータ）を埋め込んだ画像データ等を、圧縮のために量子化しても、埋め込まれた認証データが失われないようにした画像処理装置およびその方法に関する。

【０００２】

【従来の技術】例えば、国際公開ＷＯ９７／４９２３５号公報（文献１）は、ピクセル・ブロック・コーディング（Pixel Block Coding；ＰＢＣ）により、画像データ等のコンテンツデータに著作権情報など（以下、一般的に認証情報あるいは埋め込みデータ等とも記す）を、視覚的に感知できないように埋め込む方式（以下、このようにコンテンツデータに感知できないように認証方法を埋め込む方式を「エレクトロニックウォーターマーキング方式」とも記す）を開示する。

【０００３】また、国際公開ＷＯ９８／１１６９２８号公報（文献２）は、文献１等に開示されたエレクトロニックウォーターマーキング方式を応用して、画像データの改変を禁止し、著作物を有効に保護する方法を開示する。また、特開平１０－１６４５４９号公報（文献３）は、文献１等に開示されたエレクトロニックウォーターマーキング方式を改良し、画像データに認証情報を一体不可分に埋め込むことにより、画像データの改変を検出する方法を開示する。

【０００４】また、これらの文献の他、特開平０９－１５１７４７号公報、特開平１０－８３３１０号公報、特開平１０－１０６１４９号公報、特開平１０－１６１９３３号公報、特開平１０－１６４３４９号公報、特開平１０－２８５５６２号公報、特開平１０－３３４２７２号公報、特開平１０－２４０６２６号公報、特開平１０－２４０１２９号公報（文献４～１２）等も、エレクトロニックウォーターマーキング方式に関する発明を開示する。

【０００５】しかしながら、これらの文献に開示された方式は、認証情報を埋め込んだ後の画像データの圧縮符号化を充分に考慮していなかった。つまり、これらの方式により埋め込まれた認証情報が量子化値より少ない場合には、埋め込まれた画像データが量子化の結果、消失してしまう可能性がある。

【０００６】

【発明が解決しようとする課題】本発明は、上述した従来技術の問題点に鑑みてなされたものであり、圧縮符号化に適した画像処理装置およびその方法を提供することを目的とする。特定的には、本発明は、認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがない画像処理装置およびその方法を提供することを目的とする。

【０００７】

【課題を達成するための手段】上記目的を達成するために、本発明にかかる画像処理装置は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換手段と、画像データに対して前記所定の処理を行う処理手段と、前記所定の処理がなされた画像データを量子化処理する量子化手段とを有する。

【０００８】好適には、前記処理手段は、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い、前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出手段をさらに有する。

【０００９】好適には、前記変換手段は、画像データに含まれる画素それぞれの形式を変換する形式変換手段と、前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節手段とを有し、前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す。

【００１０】好適には、前記処理手段は、前記画像データに対して埋込データを埋め込む埋込処理を前記所定の処理として行う。

【００１１】好適には、前記処理手段は、所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算手段と、計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理手段とを有する。

【００１２】好適には、前記画像データに埋め込まれた埋込データを検出する検出手段をさらに有する。

【００１３】好適には、前記量子化された画像データを逆量子化する逆量子化手段と、前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出手段と、前記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算手段と、前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出手段とを有する。

【００１４】また、本発明にかかる画像処理方法は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換し、画像データに対して前記所定の処理を行い、前記所定の処理がなされた画像データを量子化処理する。

【００１５】また、本発明にかかる記録媒体は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換ステップと、画像データに対して前記所定の処理を行う処理ステップと、前記所定の処理がなされた画像データを量子化処理する量子化ステップとをコンピュータに実行させる

プログラムを記録する。

【0016】

【発明の実施の形態】［第1実施形態］以下、本発明の第1実施形態を説明する。

【0017】［改変判定装置1］図1は、本発明にかかる画像処理方法を実現する画像処理装置1の構成を示す図である。図1に示すように、画像処理装置1は、CRT表示装置あるいは液晶表示装置等の表示装置100、キーボードおよびマウス等を含む入力装置102、ディジタルカメラインターフェースIF（カメラIF）104、メモリカードインターフェース（メモリカードIF）106、MO装置およびCD装置等の記憶装置108、および、メモリ112およびマイクロプロセッサ（CPU）114等を含むコンピュータ本体（PC本体）110から構成され、必要に応じて、さらに通信装置116が付加される。つまり、画像処理装置1は、一般的なコンピュータに、カメラIF104およびメモリカードIF106を付加した構成を採る。

【0018】画像処理装置1は、これらの構成部分により、ディジタルカメラ140が撮影した画像データ（JPEG、BMPあるいはYUVなど形式を問わない）を、カメラIF104を介して受け入れる。あるいは、画像処理装置1は、ディジタルカメラ140がメモリカード142に記録した画像データを、メモリカードIF106を介して受け入れる。

【0019】さらに、画像処理装置1は、光磁気ディスク（MO）あるいはコンパクトディスク（CD）等の記録媒体120に記録されて記憶装置108に供給される埋込・検出プログラム2（図2等を参照して後述する）を、メモリ112にロードして実行し、受け入れた画像データに対して、量子化処理しても失われることがないように電子透かし（埋め込みデータ）の埋め込み処理を行う。

【0020】また、画像処理装置1は、埋込・検出プログラム2を実行し、画像データに埋め込まれた電子透かしを検出し、画像データに対して改ざんが加えられたか否かを判定する。

【0021】［埋込・検出プログラム2］まず、埋込・検出プログラム2の構成および動作を説明する。図2は、図1に示した画像処理装置1が実行し、本発明にかかる画像処理方法を実現する埋込・検出プログラム2の構成を示す図である。図2に示すように、埋込・検出プログラム2は、OS80、埋込・抽出部3、鍵情報データベース（DB）22および画像データベース（DB）24から構成される。埋込・抽出部3は、埋込パラメータDB20、制御部26、埋込部30および抽出部40から構成される。

【0022】［OS80］OS80は、例えば、OS／2（IBM社）あるいはウィンドウズ（マイクロソフト社）等のオペレーティングシステムソフトウェアであって、埋込・検出プログラム2の各構成部分の実行制御を行う。

【0023】［制御部26］埋込・抽出部3の制御部26は、例えば、表示装置100に操作用のGUI画像（図示せず）を表示し、表示されたGUI画像に対するユーザの操作を受け入れ、必要に応じて、受け入れた操作を示す操作データを、埋込・検出プログラム2の各構成部分に供給する。また、制御部26は、受け入れたユーザの操作に応じて、埋込・検出プログラム2の各構成部分の動作を制御する。

【0024】［画像DB24］画像DB24は、埋込部30が電子透かしを埋め込んだ圧縮画像データ（JPEGデータ）を記憶装置108に挿入された記録媒体120、あるいは、メモリカードIF106に挿入されたメモリカード142に記憶・管理し、記憶・管理した画像データを読み出して抽出部40に対して出力する。

【0025】［鍵情報DB22］鍵情報DB22は、画像DB22が管理するJPEGデータと、埋込部30が、このJPEGデータへ電子透かしを埋め込む際に、乱数を発生させるために用いる鍵（例えば64ビットの数値）とを対応付けた鍵情報を記憶装置108等に記憶・管理し、記憶・管理した鍵情報を読み出して埋込部30および抽出部40に対して出力する。

【0026】［埋込パラメータDB20］埋込パラメータDB20は、電子透かしの埋め込みに用いるパラメータを記憶・管理し、埋込部30に対して出力する。

【0027】［埋込部30］図3は、図2に示した埋込部30の構成を示す図である。図4は、注目DCT係数を示す図である。図3に示すように、埋込部30は、埋込前処理部32、ハッシュ（Hash）値計算部300、ハッシュ値埋込部302および出力フォーマット変換部304から構成される。埋込部30は、これらの構成部分により、まず、各種（JPEG、RGB（ビットマップ（BMP））および輝度・色差（YUV）等）の形式の画像データから、予め定められたハッシュ関数とキーとを用いて、注目するDCT（図4）係数のハッシュ値を計算する。

【0028】さらに、埋込部30は、計算の結果として得たハッシュ値を、画像データ自体に対して電子透かしの手法を用いて埋め込む、あるいは、画像データのヘッダ部分に埋め込む等の方法により、画像データに付加する。なお、埋込部30を画像データのY，U，V各成分から得られたDCT係数に対して、電子透かしの手法を用いてハッシュ値を埋め込むように構成することも、Y，Cr，Cb各成分から得られたDCT係数に対してハッシュ値を埋め込むように構成することも可能であるが、説明の明確化のために、以下、埋込部30が、計算して得たハッシュ値を、画像データのY，U，V各成分から得られたDCT係数に対して埋め込む場合を具体例とする。

【００２９】［埋込前処理３２］図５は、図３に示した埋込前処理部３２の構成を示す図である。また、図５に示すように、埋込パラメータＤＢ２０（図２）の埋込前処理３２は、フォーマット認識部３２０、逆量子化部（Q-1）３２２、量子化値計算部３２４、ＪＰＥＧ’／ＢＭＰ変換部３２６、ＹＵＶ／ＢＭＰ変換部３２８、ＢＭＰ／ＪＰＥＧ’変換部３３０およびＤＣＴ係数調整部３３２から構成される。

【００３０】埋込部３０は、これらの構成部分により、ＤＣＴ変換してハッシュ値を埋め込んで電子透かしを埋め込み、さらに、圧縮符号化してＪＰＥＧ形式の圧縮画像データ（ＪＰＥＧデータ）とした場合であっても、埋め込んだハッシュ値が失われない状態（安定状態）になるように、画像データ（ＢＭＰデータ）に対して埋込前処理を行う。

【００３１】［フォーマット認識部３２０］埋込前処理３２において、フォーマット認識部３２０は、入力された各種形式の画像データ（ＪＰＥＧデータ，ＢＭＰデータ，ＹＵＶ形式の画像データ（ＹＵＶデータ）等）のデータフォーマットを識別し、入力された画像データがいずれの形式であるかを判断し、ＪＰＥＧデータが入力された場合には、入力されたＪＰＥＧデータを復号部３２２に対して出力し、ＢＭＰデータが入力された場合には、入力されたＢＭＰデータをＢＭＰ／ＪＰＥＧ’変換部３３０に対して出力し、ＹＵＶデータが入力された場合には、入力されたＹＵＶデータをＹＵＶ／ＢＭＰ変換部３２８に対して出力する。

【００３２】さらに、フォーマット認識部３２０は、ＢＭＰデータにおいてハッシュ値を埋め込む領域を、例えば１６×１６画素構成のＭＣＵ単位で指定する領域指定データＡを受け、領域指定データＡが示すＭＣＵそれぞれに含まれるＤＣＴ係数が安定状態であるか否かを示すＭＣＵテーブルＴ（Ｔ［Ｘ］［Ｙ］、例えば、ＢＭＰデータが７２０×４８０画素構成である場合にはＸ＝４５，Ｙ＝３０）を作成する。

$$T[X][Y]=\begin{cases}1 & :(X,Y)\in A\text{の場合}\\ 0 & :(X,Y)\notin A\text{以外の場合}\end{cases}\qquad(1)$$

【００３３】なお、領域指定データＡにより指定される領域は、ＪＰＥＧ’／ＢＭＰ変換部３２６およびＹＵＶ／ＢＭＰ変換部３２８による変換処理の対象とはならない。画質に与える影響を最小にすることができるという意味で、領域指定データＡを、画面の端の領域を指定するように作成すると、そうでない場合に比べてより好適である。フォーマット認識部３２０は、作成したＭＣＵテーブルＴを、ＪＰＥＧデータ、ＢＭＰデータおよびＹＵＶデータそれぞれに付して、復号部３２２、ＢＭＰ／ＪＰＥＧ’変換部３３０およびＹＵＶ／ＢＭＰ変換部３２８にそれぞれに対して出力する。

【００３４】上述のように、ＭＣＵテーブルＴは、例えば４５×３０のマトリクス形式で表され、ＭＣＵテーブルＴの各要素Ｔ［Ｘ］［Ｙ］はそれぞれは、例えば、対応するＭＣＵのＤＣＴ係数データが安定状態である場合には値１、安定でない場合には値０を採る。フォーマット認識部３２０は、下式１に示すように、ＭＣＵテーブルＴの初期値として、領域指定データＡが示すＭＣＵに対応するＭＣＵテーブルＴの要素Ｔ［Ｘ］［Ｙ］の値を１とし、これら以外のＭＣＵテーブルの要素Ｔ［Ｘ］［Ｙ］の値を０とする。

【００３５】

【数１】

$$T[X][Y]=\begin{cases}1 & :(X,Y)\in A\text{の場合}\\ 0 & :(X,Y)\notin A\text{以外の場合}\end{cases}\qquad(1)$$

【００３６】［復号部３２２］ＪＰＥＧデータは、ＤＣＴ係数に対して量子化処理およびハフマン（Huffman）符号化処理を施すことにより生成される。復号部３２２は、まず、フォーマット認識部３２０から入力されたＪＰＥＧデータをハフマン復号する。また、復号部３２２は、復号したＪＰＥＧデータのＹ，Ｕ，Ｖ各成分からそれらの量子化値ｑ［ｋ］を計算し、埋込量子化値計算部３２４に対して出力する。また、復号部３２２は、計算の結果として得た量子化値ｑ［ｋ］それぞれを用いて、ハフマン復号したＪＰＥＧデータのＹ，Ｕ，Ｖ各成分を逆量子化して、Ｙ，Ｕ，Ｖ各成分のＤＣＴ係数ＪＰＥＧ’を生成し、ＭＣＵテーブルＴと対応づけてＪＰＥＧ’／ＢＭＰ変換部３２６に対して出力する。

【００３７】［ＹＵＶ／ＢＭＰ変換部３２８］ＹＵＶ／ＢＭＰ変換部３２８は、ＹＵＶデータを、下式２に示す

$$\begin{aligned}R&=(\mathrm{int})(Y+V*1.4020)\\ G&=(\mathrm{int})(Y-U*0.3441-V*0.7139)\\ B&=(\mathrm{int})(Y+U*1.7718-V*0.0012)\end{aligned}\qquad(2)$$

但し、

$$R=R>255\ ?\ 255:R<0\ ?\ 0:R$$

```
G = G>255 ? 255 : G<0 ? 0 : G
B = G>255 ? 255 : B<0 ? 0 : B
```

ここで、A＝　B？C：Bは、C codeのものと同じで、

```
A= C (if B is TRUE)
A= D (if B is NOT TRUE)
```

である。

【００３９】［ＪＰＥＧ’／ＢＭＰ変換部３２６］ＪＰＥＧ’／ＢＭＰ変換部３２６は、復号部３２２およびＤＣＴ係数調整部３３２から入力されるＤＣＴ係数ＪＰＥＧ’の内、領域指定データAが示す領域以外のＭＣＵのＹ，Ｕ，Ｖ成分それぞれのＤＣＴ係数を逆ＤＣＴ（ＩＤＣＴ）処理する。ＪＰＥＧ’／ＢＭＰ変換部３２６は、さらに、ＩＤＣＴ処理の結果として遷られたＹ，Ｕ，Ｖ成分を、ＹＵＶ／ＢＭＰ変換部３２８と同様に上記式２に従ってＢＭＰデータに変換し、ＭＣＵテーブルＴと対応づけてＢＭＰ／ＪＰＥＧ’変換部３３０に対して出力する。

【００４０】［ＢＭＰ／ＪＰＥＧ’変換部３３０］ＢＭ

```
Y =  R*0.2990 + G*0.5870 +B*0.1140
U = -R*0.1684 - G*0.3316 +B*0.5000
V =  R*0.5000 - G*0.4187 -B*0.0813
```

【００４２】［埋込量子化値計算部３２４］埋込量子化値計算部３２４は、領域指定データAにより示されるＤＣＴ係数（注目ＤＣＴ係数）ｄｃｔ＿Ｃｏｅｆｆｉの埋込量子化値ｑ＿ｅｍｂ［ｋ］を算出する。さらに埋込量子化値計算部３２４の処理を詳細に説明する。埋込量子化値計算部３２４は、注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉおよびデコーダ最大計算誤差δを、埋込パラメータＤＢ２０（図２）から受ける。

【００４３】［注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉ］ここでは、注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉを詳細に説明する。注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉは、電子透かしの埋め込みに用いる８×８画素構成のＤＣＴブロックに含まれる１つ以上のＤＣＴ係数であり、Ｙ，Ｕ，Ｖ成分のいずれのＤＣＴ係数であってもよいが、以下、説明の明確化のために、注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉとしてＹ成分のＤＣＴ係数の内の直流成分ｄｃｔ＿ｃｏｅｆｆｉ（０，０）を用い、ハッシュ値の埋め込みのために、同じくＹ成分のＤＣＴ係数の内の（１，１），（１，２），（２，１），（２，２）を利用する場合を具体例とする。

【００４４】［デコーダ最大計算誤差δ］ここでは、デコーダ最大計算誤差δを詳細に説明する。また、ハッシュ値を埋め込んだＪＰＥＧデータを伸長復号処理するデコーダが違う場合には、システム間でＩＤＣＴ処理の結果に誤差が生じる可能性がある。デコーダ最大計算誤差δは、埋め込み量子化値：システム(decoder)の違いから生じるＩＤＣＴ処理の誤差の２倍の値に設定される。な

```
q_emb[k] = (int((δ-1)/q[k]+1)*q[k]
```

【００４８】なお、量子化値ｑ［ｋ］がデコーダ最大計算誤差δよりも大きい場合（ｑ［ｋ］≧δ）、埋込量子化値計算部３２４は、領域指定データAが示す注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉそれぞれに対応する埋込量子化値ｑ＿ｅｍｂ［ｋ］（ｋ（｛ｄｃｔ＿ｃｏｅｆｆｉ｝））を、下式４に示すように計算する。なお、埋込量子化値ｑ＿ｅｍｂ［ｋ］は、ハッシュ値を埋め込んだＤＣＴ係数を量子化処理するために用いられる量子化値であって、量子化値ｑ［ｋ］の整数倍の値を採る。

【００４７】

【数４】

（４）

【数３】

（３）

お、ＩＤＣＴ処理の誤差は、ほとんどの場合、２以下である。従って、デコーダ最大計算誤差δの設定値は４以上あれば充分である。以下、デコーダ最大計算誤差δの値を、充分に大きい１２に設定する場合を具体例として説明する。

【００４５】埋込量子化値計算部３２４は、埋込前処理３２に入力された画像データがＪＰＥＧデータである場合には、復号部３２２から入力された量子化値ｑ［ｋ］を、ＪＰＥＧデータでない場合には、例えば、入力装置１０２を介してユーザが入力する量子化値ｑ［ｋ］を用いて以下の処理を行う。なお、埋込量子化値計算部３２４は、例えば、埋込前処理３２に入力された画像データがＪＰＥＧデータでなく、しかも、入力装置１０２から量子化値ｑ［ｋ］の入力がない場合には、量子化値ｑ［ｋ］の全ての要素の値をデコーダ最大計算誤差δに設定する（ｑ［ｋ］＝δ）。

【００４６】次に、埋込量子化値計算部３２４は、領域指定データAが示す注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉそれぞれに対応する埋込量子化値ｑ＿ｅｍｂ［ｋ］（ｋ（｛ｄｃｔ＿ｃｏｅｆｆｉ｝））を、下式４に示すように計算する。なお、埋込量子化値ｑ＿ｅｍｂ［ｋ］は、ハッシュ値を埋め込んだＤＣＴ係数を量子化処理するために用いられる量子化値であって、量子化値ｑ［ｋ］の整数倍の値を採る。

【００４７】

【数４】

（４）

算誤差δよりも大きい場合（ｑ［ｋ］≧δ）、埋込量子

化値ｑ＿ｅｍｂ［ｋ］と量子化値ｑ［ｋ］とは一致する（ｑ＿ｅｍｂ［ｋ］＝ｑ［ｋ］）。また、埋込前処理３２にＪＰＥＧデータが入力される場合、量子化値ｑ［ｋ］の変更は不要である。

【００４９】［ＤＣＴ係数調整部３３２］ＤＣＴ係数調整部３３２は、ＪＰＥＧ’／ＢＭＰ変換部３２６、ＢＭＰ／ＪＰＥＧ’変換部３３０およびＤＣＴ係数調整部３３２により構成されるループ処理を制御し、このループ処理を所定の回数（例えば５回）繰り返して、ＢＭＰ／ＪＰＥＧ’変換部３３０から入力された注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉが、埋込量子化値ｑ＿ｅｍｂ［ｋ］の整数倍に近い値をとるように、つまり、注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉが安定状態になるようにそれらの値を調整する。

【００５０】以下、さらにＤＣＴ係数調整部３３２の処理を詳細に説明する。ＤＣＴ係数調整部３３２は、埋込パラメータＤＢ２０（図２）から安定化閾値Δを受け

$$|c[k] - coeff\_emb[k]*q\_emb[k]| < \Delta/2 \qquad (5)$$

【００５３】ＤＣＴ係数調整部３３２は、全てのＭＣＵの全てのＤＣＴブロックに含まれるＤＣＴ係数が式５を満し、安定状態になっている場合には、注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉおよびその他のＤＣＴ係数を画像ＤＢ２４（図２）に対して出力し、安定状態になっていない場合には、安定状態になっていないＤＣＴ係数が安定状態になるように調節する。なお、ＤＣＴ係数調整部３３２は、ｃｏｅｆｆｉ＿ｅｍｂ［ｋ］を、領域指定データＡが示す注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉとして、それ以外のＤＣＴ係数は、量子化処理した値（ｃｏｅｆｆｉが、埋込量子化値ｑ＿ｅｍｂ［ｋ］の整数倍に近い値になっているか否かを判断するために用いられる閾値であって、例えばデコーダ最大計算誤差σよりも小さい値、例えば１程度の値に設定される（$\delta > \Delta = 1.0$）。

【００５１】ＤＣＴ係数調整部３３２は、次に、領域指定データＡにより示されるＭＣＵのＤＣＴブロックそれぞれに含まれる各ＤＣＴ係数が、下式５を満たしている否かを判断する。ＤＣＴ係数調整部３３２は、判断対象のＤＣＴブロックに含まれるＤＣＴ係数のすべてが下式５を満たしている場合には、このＤＣＴブロックに対応するＭＣＵテーブルＴの要素Ｔ［Ｘ］［Ｙ］の値を安定状態を示す１とし（Ｔ［Ｘ］［Ｙ］＝１）、これ以外の場合には０とする（Ｔ［Ｘ］［Ｙ］＝０）。

【００５２】

【数５】

ｅｆｆｉ［ｋ］＝ｃ［ｋ］／ｑ［ｋ］）を、画像ＤＢ２４（図２）に対して出力する。

【００５４】［ＤＣＴ係数の安定化］ここでは、ＤＣＴ係数調整部３３２がＤＣＴ係数を安定状態にする処理（安定化処理）を詳細に説明する。ＤＣＴ係数調整部３３２は、値が０のＭＣＵテーブルＴの要素Ｔ［Ｘ］［Ｙ］に対応するＭＣＵのＤＣＴ係数を、下式６に示すように変換する。

【００５５】

【数６】

$$c[k] = coeff\_emb[k] * q\_emb[k] \quad : \quad if\ k \in \{dct\_coeffi\}$$

$$c[k] = (int)(c[k]>0\ ?\ c[k]/q[k]+\alpha\ :\ c[k]<0\ ?\ c[k]/q[k]-\alpha\ :\ 0)*q[k] \quad otherwise$$

但し、

$$coeff\_emb[k] = (int)(c[k]>0\ ?\ c[k]/q\_emb[k]+\alpha\ :\ c[k]<0\ ?\ c[k]/q\_emb[k]-\alpha\ :\ 0) \qquad (6)$$

【００５６】式６において、αは０～０．５の間の値を採る数値であって（$0 \leqq \alpha \leqq 0.5$）、αの値を大きくすると、安定化処理が再生画像に与える変化を小さくすることができる。しかしながら、変換後のcoeff[k]の値の絶対値は常に大きくなり、安定状態にした後のＤＣＴ係数を変換して得られるＢＭＰデータのＲ，Ｇ，Ｂ成分の値に近づくので、ＢＭＰデータのＲ，Ｇ，Ｂ成分の値にオーバーフロー・アンダーフローが生じやすい。一方、αを小さくすると、変換後のcoeff[k]の値の絶対値は常に小さくなり、安定状態にした後のＤＣＴ係数を変換して得られるＢＭＰデータのＲ，Ｇ，Ｂ成分それぞれの値は１２８に近づくので、ＢＭＰデータのＲ，Ｇ，Ｂ成分の値にオーバーフロー・アンダーフローが生じにくい。

【００５７】このようなαの性質を考慮し、安定化処理が再生画像に与える影響を極力少なくし、かつ、安定化したＤＣＴ係数を変換して得られるＢＭＰデータにオーバーフロー・アンダーフローが生じないようにするために、ＤＣＴ係数調整部３３２は、ＪＰＥＧ’／ＢＭＰ変換部３２６、ＢＭＰ／ＪＰＥＧ’変換部３３０およびＤＣＴ係数調整部３３２によるループ処理を１回行うごとに、αの値を減らしてゆくようにする。

【００５８】例えば、ＪＰＥＧ’／ＢＭＰ変換部３２６、ＢＭＰ／ＪＰＥＧ’変換部３３０およびＤＣＴ係数調整部３３２によるループ処理の回数をｌｏｏｐｃｏｕｎｔとすると、ＤＣＴ係数調整部３３２は、下式７に示すように、ループ処理の回数に応じてαの値を少なくする。

【００５９】

【数７】

$$\alpha = 0.5 \quad \text{loopcount}/10 \qquad (\text{loopcount}<5)$$
$$0 \qquad (\text{loopcount}>=5) \qquad (7)$$

【0060】DCT係数調整器332は、上述した調整を、値が0のMCUテーブル下の要素T［X］［Y］に対応するMCUに含まれるDCTブロック全てのDCT係数に対して行い、JPEG'／BMP変換部326に対して出力する。

【0061】なお、ごくまれに、JPEG'／BMP変換部326における処理でオーバーフロー・アンダーフローが生じていて、ループ処理を5回繰り返した後でも、式5の条件を満たすことがないDCT係数が存在することがある。このような場合に対応するために、DCT係数調整部332は、ループ処理を5回繰り返した後は、さらに、DCT係数の値が式5の条件を満たすようになるまでループ処理を1回ずつ追加して行い、ループ処理を1回追加するたびに、coeff_emb[k]の絶対値を1（但し、何らかの制約がある場合、その制約を満たす1以上の最小数）づつ減らす。このように、ループ処理を追加し、ループ処理1回ごとにcoeff_emb[k]の絶対値を1（但し、何らかの制約がある場合、その制約を満たす1以上の最小数）づつ減らすことにより、DCT係数調整部332は、画像の変化を極力少なくしつつ、ループ処理を有限回数に抑える。

【0062】以上説明した埋込前処理32の処理により、図6（A）に示すように分布していた注目DCT係数dct_coeffiの値は、図6（B）に示すように、埋込量子化値q_emb［k］の整数倍に近い値を採るようになり、埋込量子化値q_emb［k］の整数倍を中心とする広がりσ（σ<δ）の範囲内に分布するようになる。

$$\text{err}[k] = |c2[k] - \text{coeff\_emb}[k] * q\_emb[k]| >= q\_emb[k]/2 \ (>= \delta/2) \qquad (8)$$

【0063】［ハッシュ値計算部300］再び図3を参照する。以上説明した埋込前処理32（図3，4）の処理により、{dec_coeffi}の全てのDCT係数が埋め込みの量子化値q_emb［k］の整数倍の近傍に来て安定化している。即ち、上述した式5を満たしている。問題は、埋込前処理32の出力から得られるJPEGデータを、JPEG'／BMP変換部326（図5）以外BMPエンコーダにより処理して式5に示した性質が保てるか否かである。例えば、埋込前処理32（図3，4）の出力データをinput．bmp、え44以外のエンコーダで作られるBMPデータをinput2．bmpとすると、これらの違いは、JPEGデータをiDCTし、さらにYUVデータに変換し、これをBMPデータに変換する処理における計算の誤差であり、この誤差のために、2つのinput．bmpとinput2．bmpとが、下式8に示すように、量子化値を跨いでしまう可能性が高い。即ち、input．bmpから導かれたDCT係数c2［k］が、下式8を満たす可能性は小さい。

【0064】

【数8】

【0065】例えば、あるBMPエンコーダでiDCT処理結果（iDCTデータ）あるいはYUVデータをBMPデータに変換する処理を小数点第1位まで用いて計算する際に、iDCTデータの計算誤差が最悪0．05あり、iDCT処理で、係数1つにつき64回の加算または減算を行うとすると、計算誤差は最悪3．35（＝0．05×63＋3）となるが、上述したように、最大誤差δを12より大きい値にとれば、上述した式8を満たすことはない。

【0066】逆に、iDCT等の計算で少数第1位以上の誤差があるようなシステムは、誤差が大きすぎで、単なる変換だけで画像が大きく変化してしまい、使用に耐えないシステムと言える。多数のシステムを調べると、最悪で err[k]=3.0程度である。よって、全ての{dct_coeffi}に対して全てのq_emb［k］による量子化値coeff_emb［k］は、JPEGデータをBMPデータに変換する処理に耐えられることになる。そのため、coeff_emb［k］のハッシュ値を取り、その結果をJPEGデータのヘッダ部分に書き込むか、画像自体に電子透かしで埋めておけば良い。

【0067】埋め込みに使われる領域Aを除き、鍵Dから与えられる、埋め込み者、検出者で共通の鍵Kを使い、

$$\text{DCT\_hash} = \text{hash}(K,\ \text{coeff\_emb}[k]) \qquad (9)$$

【0069】なお、式9におけるhash（ ）としては、MD5などがある。また、鍵Kとしては、64ビット鍵、DCT_hashは64ビット長が妥当な長さである。

【0070】［ハッシュ値埋込部302］ハッシュ値埋込部302は、ハッシュ値計算部300で選られたDCT_hashを画像に埋め込む。画像に埋め込むアルゴリズムは何を用いてもよいが、画像を痛めない方法としてはLSB法があり、LSB法とは、電子透かしをデジタルコンテンツに埋め込む方式の1つで、コンテンツの特徴量のLSB(least significant bit、最下位bit)をある規則に従って変化させることによって、情報を埋め込む。LSBを変化させる理由は、埋め込み後のデジタルコンテンツ（画像、音）の変化が殆と無い為である。

【0071】以下、具体例を挙げて説明する。埋込パラメータDB20（図2）から得られる埋め込みに利用するDCT係数{dct_coeffi}の要素がn個あ

り、ｈａｓｈ＿ｅｍｂが６４ビットで、１つのサブブロック（８×８画素）にｍビットを埋め込む事を考える（ｎ>=ｍ）。つまり、埋め込みに６４／ｍ個のサブブロックが必要となる。

【００７２】ここで、埋め込みによる画質の痛みを極力防ぐ為に、Ａの候補を予め選つか決めておいて（例：画面の上、下、右、左端の４個所）、そのどこかに埋めて、検出時に全て試すという方法もある。さて、ここで、｛ｄｃｔ＿ｃｏｅｆｆｉ｝のＬＳＢに埋めたいｂｉｔを埋めていくわけである。

【００７３】

【数１０】

$$emb\_coeff[k] = 2p + emb\_bit[k] \qquad (10)$$

ｐはある整数、emb_bit[k]は係数kに埋めたいbit,0 or 1

【００７４】上式１０を満たすようにｅｍｂ＿ｃｏｅｆ［ｋ］を変更後、Ａの領域のみのＤＣＴ係数をＪＰＥＧ’／ＢＭＰ変換部３２６（図５）に入力し、Ａ内の全ての｛ｄｃｔ＿ｃｏｅｆｆｉ｝のＤＣＴ係数が、上式１０を満たしつつ安定になるようにすれば良い。この場合、常に、emb_coeff[k]の値の絶対値が大きくならない方向に変更していけば、つまりαを小さく取れば、取束は速く、式６が達成できる。式６が達成出来れば、Ａは安定の為、ＢＭＰデータに変換した後も、埋めたビットが変化しない。

【００７５】［出力フォーマット変換部３０４］出力フォーマット変換部３０４は、ハッシュ値埋込部３０２の出力結果に対して量子化処理などを行い、入力装置１０２（図１）を介して設定されるユーザ所望の出力フォーマットに変換する。出力フォーマットがＪＰＥＧの際、｛ｄｃｔ＿ｃｏｅｆｆｉ｝に属するＤＣＴ係数も、ｑ＿ｅｍｂ［ｋ］ではなく、ｑ［ｋ］で量子化する。ｑ［ｋ］で量子化された値ｃｏｅｆｆ［ｋ］は、ｅｍｂ＿ｃｏｄｆｆ［ｋ］，ｑ［ｋ］，ｑ＿ｅｍｂ［ｋ］より、coeff[k] = emb_coeff[k]*q_emb[k]/q[k]によって計算される。

【００７６】［検出部４０］以下、検出部４０（図２）を説明する。埋め込み装置で埋め込まれた画像データを入力し、鍵Ｋより注目するＤＣＴ成分のハッシュ値を計算し、領域Ａに埋め込まれているハッシュ値と比較し、画像自体が改ざんされたかどうかを検出する。

【００７７】［検出前処理部４２］図７は、図２に示した検出部４０の構成を示す図である。図８は、図７に示した検出前処理部４２の構成を示す図である。検出部４０において、検出前処理部４２は、入力画像より埋め込み量子化値ｑ＿ｚｍｂ［ｋ］を逆算する。

【００７８】［フォーマット認識部４２０］フォーマット認識部４２０は、入力画像のフォーマットを認識し、ＪＰＥＧなら復号部４２２に対して出力し、ＢＭＰ，ＹＵＶならＢＭＰ，ＹＵＶ／ＪＰＥＧ’変換部４２４に対して出力する。

【００７９】［復号部４２２］復号部４２２は、入力画像を復号し、Ａを除く画像全体の注目するＤＣＴ成分の係数を逆量子化して、ＪＰＥＧ’画像とする。

【００８０】［ＢＭＰ，ＹＵＶ／ＪＰＥＧ’変換部４２４］ＢＭＰ，ＹＵＶ／ＪＰＥＧ’変換部４２４は、入力されたＢＭＰ，ＹＵＶデータをＤＣＴ処理し、ＪＰＥＧ’データに変換する。

【００８１】［量子化値逆算部４２６］

【００８２】図９および図１０は、図８に示した量子化値逆算部４２６における埋め込み量子化値逆算処理を示す第１および第２のフローチャートである。量子化値逆算部４２６は、復号部４２２およびＢＭＰ，ＹＵＶ／ＪＰＥＧ’変換部４２４の出力の注目するＤＣＴ成分ｋ∈｛ｄｃｔ＿ｃｏｅｆｆｉ｝の画像全体での絶対値の最大係数をｍａｘ［ｋ］として、各々の仮定した量子化値ｉの回りにどのくらいＤＣＴ係数が集まっているかのヒストグラムからに示すように計算する。図９に示すように、フォーマット認識部４２０への入力フォーマットがＪＰＥＧの場合、ｉ＝ｑ［ｋ］＊ｎ（ｎ＝１，２，．．．．）に対してのみ調べれば良い。

【００８３】図９に示した処理により求められたヒストグラム［ｉ］の最大値を与えるｉを、ｍａｘ＿ｉとおき、図１０に示した処理にしたがって、ｑ＿ｅｍｂ［ｋ］を決定する。図１０では、図９でｑ＿ｅｍｂ［ｋ］が、ｍａｘ＿ｉの倍数であることからｑ＿ｅｍｂ［ｋ］を求めている。

【００８４】ここで、Ｔ＿ｔｈｒｅは１より少し小さい値で、Ｔ＿ｔｈｒｅ＝０．８辺りが妥当である。ここで、Ｔ＿ｔｈｒｅの値の精度等より図９および図１０に示した処理によりうまくｑ＿ｅｍｂ［ｋ］が求められない例外的な画像に関して、埋め込み処理の過程において、図９および図１０に示した処理により、正しくｑ＿ｅｍｂ［ｋ］が満たされるようなヒストグラムになるようにすればよい。例えば、ｑ＿ｅｍｂ［ｋ］＊２ｎの周りに多く係数が集まってしまうような場合、画像全体のうち、痛みが少なそうなところで、ｑ＿ｅｍｂ［ｋ］＊２ｎ＋１に埋め込むようにすれば良い。

【００８５】［ハッシュ値抽出部４００］再び図７を参照する。ハッシュ値抽出４００は、埋め込み領域Ａにおいて、埋込パラメータＤＢ２０からの埋め込みＤＣＴ成分｛ｄｃｔ＿ｃｏｅｆｆｉ｝の係数ｃ［ｋ］と、検出前処理部４２によって計算された、埋め込み量子化値ｑ＿ｅｍｂ［ｋ］より、以下の方法でＬＳＢをしらべ、それらを並べて埋め込まれたハッシュ値ｅｍｂｅｄ＿ｈａｓｈを計算する。

【００８６】

【数１１】

$$LSB = (int)((c[k]+\beta)/q\_emb[k]) \bmod 2$$

但し、β = c[k]>=0 ? q_emb[k]/2 ： -q_emb[k]/2　　（１１）

【００８７】［ハッシュ値計算部４０２］ハッシュ値計算部４０２は、A以外の領域に対して、｛ｄｃｔ＿ｃｏｅｆｆｉ｝の係数Ｃ［ｋ］ｑ＿ｅｍｂ［ｋ］より、上記式６においてでα=0.5として、ｃｏｅｆｆ＿ｅｍｂ［ｋ］を求め、上記式９によりＤＣＴ＿ｈａｓｈを計算する。

【００８８】［改ざん検出部４０４］改ざん検出部４０４は、ハッシュ値検出４００およびハッシュ値計算部４０２から得られるＤＣＴ＿ｈａｓｈ，ｅｍｂｅｄ＿ｈａｓｈが、ＤＣＴ＿ｈａｓｈ＝＝ｅｍｂｅｄ＿ｈａｓｈなら改ざんなし、それ以外の場合（ＤＣＴ＿ｈａｓｈ≠ｅｍｂｅｄ＿ｈａｓｈ）には改ざん有りとして、表示装置１００（図１）等に表示する。

【００８９】［全体動作］図１１は、埋込・検出プログラム２（図２）による埋め込み処理を示すフローチャートである。図１２は、埋込・検出プログラム２（図２）による検出処理を示すフローチャートである。なお、図１１および図１２の各処理中の括弧内の番号は、その処理を行う埋込・検出プログラム２の構成部分（図３，５，７，８）に付された符号を示す。埋込・検出プログラム２の各構成部分は、図１１に示すように検出込み処理を行い、図１２に示すように検出処理を行う。

【００９０】［変形例］以下、本発明に係る埋め込み装置の変形例を説明する。図１３は、埋込・検出プログラム２（図２）において埋込部３０の代わりに用いられる埋込部５０の構成を示す図である。図１４は、図１３に示した埋込前処理部５２の構成を示す図である。図１５は、図１３に示した改ざんマーク埋込部５４の構成を示す図である。

R=LFSRb(K,R0)

【００９６】［合成部５４４］合成部５４４は、データを埋め込む場合に、埋め込みデータとRより埋め込みbit列R'を合成して作成する。なお、合成部５４４が、改ざんマークを埋め込む場合、R'=Rとなる。データを埋め込む場合は、下式１３により示されるR'が埋め込みbitになる。ここで、^はxorを意味する。但し、dataは540

R' = R ^ data

【００９８】［ＬＳＢ操作部５４６］ＬＳＢ操作部５４６は、R'とｑ＿ｅｍｂ［ｋ］，ｃ［ｋ］，ｋ，（ｘ，ｙ）より，｛ｄｃｔ＿ｃｏｅｆｆｉ｝に属するＤＣＴ係数のＬＳＢを操作する。先ず、埋め込みビットｅｍｂ＿ｂｉｔ［ｋ］は、下式１４を埋め、あとは、上記式１０

emb_bit[k] = (R'>>(xn+90yn+1))&1

【０１００】［ＤＣＴ成分分割部５２８］ＤＣＴ成分分割部５２８は、復号部５２２およびＢＭＰ，ＹＵＶ／ＪＰＥＧ’変換部５２４から入力されるＤＣＴ係数(量子化されていない)を注目ＤＣＴ(｛ｄｃｔ＿ｃｏｅｆｆｉ｝)とそうでないものに分ける。

【０１０１】［量子化値計算部５２６］量子化値計算部

【００９１】なお、埋込部５０の構成部分の内、出力フォーマット変換部５０２は、埋込部３０（図３）の出力フォーマット変換部３０４に同じであり、埋込前処理部５２の構成部分の内、フォーマット認識部５２０、復号部５２２、ＢＭＰ，ＹＵＶ／ＪＰＥＧ’変換部５２４、量子化値変換部５２６および量子化値計算部５２６は、それぞれ埋込前処理３２（図５）のフォーマット認識部３２０、復号部３２２、ＪＰＥＧ’／ＢＭＰ変換部３２６、ＹＵＶ／ＢＭＰ変換部３２８および埋込量子化値計算部３２４に同じである。また、埋込部５０においては領域Aは存在しない。

【００９２】［埋め込み前処理部５２］埋込前処理部５２は、入力画像より、ＤＣＴ係数を抽出する。

【００９３】［改ざんマーク埋め込み部５４］改ざんマーク埋込部５４は、改ざんマークあるいはデータを埋め込む部分で、埋め込みアルゴリズムは何でも良く、画像を痛めない方法としてはＬＳＢ法がある。

【００９４】［画像分割部５４０］画像を８×８画素のブロック（イントラブロック）単位に分割し、入力注目ＤＣＴ成分I,係数c[k]と画像位置(x,y)を出力する。

【００９５】［乱数発生部５４２］乱数発生部５４２は、鍵Ｋより乱数Ｒを発生させる。Ｒは、埋め込みに必要なbit数だけのbitが必要で、720x480画素の場合、90x60xn = 5400n bit以上である必要がある。Bの作成方法は色々あるが、LFSRを使う場合、b=(int)(1+log25400n)bitのLFSRを使って、Kをkey,R0を鍵DBより得られる初期値（鍵の１部と考えても良い）、LFSRbをb bitのLFSR計算部として、下式１２により求められる。

【数１２】

（１２）

0n bitの埋め込みdataで、埋め込みたいdataがn bitで、m<5400n bitの場合、埋め込みdataをm周期で繰り返し、5400n/m回繰り返して埋める、等の方法もある。

【００９７】

【数１３】

（１３）

を満たすように、｛ｄｃｔ＿ｃｏｅｆｆｉ｝に属する全てのDCT係数をＴ［ｘ］［ｙ］＝０を満たす全てのＭＣＵに対して行う。

【００９９】

【数１４】

（１４）

５２６は、上述したように埋込量子化値計算部３２４と同じである。但し、Ｔ［４５］［６０］を、初期状態（Ｔ［ｘ］［ｙ］＝０、ｆｏｒａｌｌ　ｘ，　ｙ）で出力する。

【０１０２】図１６は、図１５に示した埋込後処理部５６の構成を示す図である。なお、埋込後処理部５６の構

成部分の内、ＤＣＴ係数調整５６４は、埋込前処理３２のＤＣＴ係数調整部３３２（図５）と同じである。

【０１０３】［ＪＰＥＧ’／ＢＭＰ変換部５６０］ＪＰＥＧ’／ＢＭＰ変換部５６０は、入力されたＪＰＥＧ’画像をｉＤＣＴ変換して、オーバーフロー／アンダーフロー処理をして、ＢＭＰフォーマットの画像に変換する。

【０１０４】［ＢＭＰ／ＪＰＥＧ’変換部５６２］ＢＭＰ／ＪＰＥＧ’変換部６００は、入力ＢＭＰ画像をＤＣＴ変換し、ＪＰＥＧ’フォーマットの画像に変換する。

【０１０５】図１７は、埋込・検出プログラム２（図２）において、検出部４０の代わりに用いられる検出部６０の構成を示す図である。検出部６０は、図１３～１６に示した検出部４０により埋め込まれた画像データが、データ埋め込みでなく、改ざんマークを埋め込みである場合、その画像の改ざんの有無を検出し、改ざん場所を８×８画素のブロック単位で特定する。｛ｄｃｔ＿ｃｏｅｆｆｉ｝の要素がｎ個ある場合、各々の８×６画素構成のブロック（イントラブロック）の改ざん検出率は$1-2^{-n}$であり、本発明例の様にn=4の場合、その確率は93.75%である。

【０１０６】［検出前処理部６００］検出前処理部６００は、図７に示した検出前処理部４２と同じである。但し、埋込領域Ａはない。

$$x = (\mathrm{int})(p/n) \bmod 90$$
$$y = (\mathrm{int})(p/n/90)$$

【０１１１】［出力フォーマット変換部６０８］出力フォーマット変換部６０８は、画像ＤＢ２４より入力した画像を、改ざん場所がわかるように変化させて出力する。

【０１１２】［全体動作］図１８および図１９は、検出部４０および検出部６０の処理を示すフローチャートであり、図中の括弧内の番号は、各処理を行う構成部分の符号を示す。検出部４０および検出部６０は、図１８に示すように埋め込み処理を行い、図１９に示すように検出処理を行う。

【０１１３】

【発明の効果】上述したように、本発明にかかる画像処理装置およびその方法は、圧縮符号化に適している。特定的には、本発明にかかる画像処理装置およびその方法によれば、認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがない。

【図面の簡単な説明】

【図１】本発明にかかる画像処理方法を実現する画像処理装置の構成を示す図である。

【図２】図１に示した画像処理装置が実行し、本発明にかかる画像処理方法を実現する埋込・検出プログラムの構成を示す図である。

【図３】図２に示した埋込部の構成を示す図である。

【図４】注目ＤＣＴ係数を示す図である。

【０１０７】［埋め込みデータ抽出部６０２］埋込データ抽出部６０２は、｛ｄｃｔ＿ｃｏｅｆｆｉ｝の要素のＤＣＴ係数のＬＳＢを抽出し、埋め込みデータを抽出する。イントラロケーション（ｘ，ｙ）（0<=x<60,0<=y<90），｛ｄｃｔ＿ｃｏｅｆｆｉ｝の要素数ｎのＬＳＢを式１１により計算し、それを(xn+90yn+1)bit目に持つ5400nbitの抽出データｅｍｂｅｄ＿ｄａｔａを計算する。

【０１０８】［埋め込みデータ計算部６０４］埋込データ計算部６０４は、図１５に示した乱数発生部５４２および合成部５４４と同じ方法で、埋め込み5400bit列Ｒ’を計算する。

【０１０９】［改ざん検出・場所特定部６０６］改ざん検出場所特定部６０６は、ｅｍｂｅｄ＿ｄａｔａ，Ｒ’から入力画像に改ざんがあったかどうか、あった場合、何処が改ざんされたかを特定する。つまり、改ざん検出場所特定部６０６は、ｅｍｂｅｄ＿ｄａｔａ＝＝Ｒ’の場合、改ざんなしと判定し、これ以外の場合（ｅｍｂｅｄ＿ｄａｔａ<>Ｒ’）には、ビット単位で値が合わない部分を全て探す。その際、例えば、ｐbit目(0 origin)が合わない場合、改ざんのあったintra location (x, y)は、以下の式によって特定出来る。

【０１１０】

【数１５】

$$\cdots \quad (15)$$

【図５】図３に示した埋込前処理部の構成を示す図である。

【図６】（Ａ）は、図３に示した埋込前処理による安定化処理の前の注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉの値の頻度をｑ［ｋ］＝３，ｑ＿ｅｍｂ［ｋ］の場合について例示し、（Ｂ）は埋込前処理による安定化処理の後の注目ＤＣＴ係数ｄｃｔ＿ｃｏｅｆｆｉの値の頻度を同様に例示するヒストグラムである。

【図７】図２に示した検出部の構成を示す図である。

【図８】図７に示した検出前処理部の構成を示す図である。

【図９】図８に示した量子化値逆算部における処理を示す第１のフローチャートである。

【図１０】図８に示した量子化値逆算部における処理を示す第２のフローチャートである。

【図１１】埋込・検出プログラム（図２）による埋め込み処理を示すフローチャートである。

【図１２】埋込・検出プログラム（図２）による検出処理を示すフローチャートである。

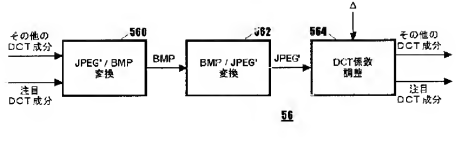
【図１３】埋込・検出プログラム（図２）において埋込部の代わりに用いられる埋込部の構成を示す図である。

【図１４】図１３に示した埋込前処理部の構成を示す図である。

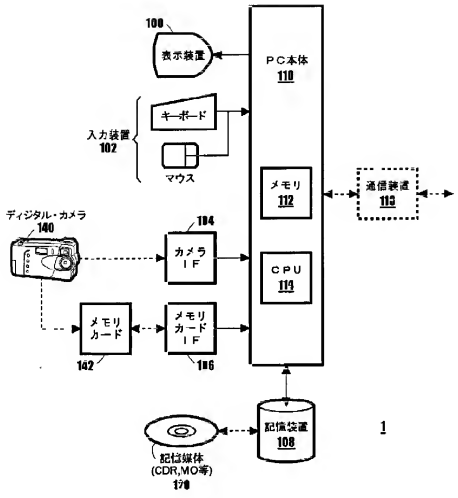
【図１５】図１３に示した改ざんマーク埋込部の構成を

示す図である。
【図16】図15に示した埋込後処理部の構成を示す図である。
【図17】埋込・検出プログラム（図2）において用いられる第2の検出部の構成を示す図である。
【図18】検出部および検出器（図13～17）の処理を示す第1のフローチャートである。
【図19】検出部および検出器（図13～17）の処理を示す第2のフローチャートである。
【符号の説明】
1・・・画像処理装置
100・・・表示装置
102・・・入力装置
104・・・カメラIF
106・・・メモリカードIF
108・・・記憶装置
110・・・PC本体
112・・・メモリ
114・・・CPU
116・・・通信装置
120・・・記録媒体
140・・・ディジタルカメラ
142・・・メモリカード
2・・・埋込・検出プログラム
20・・・埋込パラメータDB
22・・・鍵情報DB
24・・・画像DB
26・・・制御部
30・・・埋込部
32・・・埋込前処理
320・・・フォーマット認識部
322・・・復号部
324・・・埋込量子化値計算部
326・・・JPEG'／BMP変換部
328・・・YUV／BMP変換部
330・・・BMP／JPEG'変換部
332・・・DCT係数調整部
300・・・ハッシュ値計算部
302・・・ハッシュ値埋込部
304・・・出力フォーマット変換部
40・・・検出部
42・・・検出前処理部
420・・・フォーマット認識部
422・・・復号部
424・・・BMP，YUV／JPEG'変換部
426・・・量子化値逆算部
400・・・ハッシュ値抽出
402・・・ハッシュ値計算部
404・・・改ざん検出部
50・・・埋込部
52・・・埋込前処理部
520・・・フォーマット認識部
522・・・復号部
524・・・BMP，YUV／JPEG'変換部
526・・・量子化値計算部
528・・・DCT成分分割部
54・・・改ざんマーク埋込部
540・・・画像分割部
542・・・乱数発生部
544・・・合成部
546・・・LSB操作部
56・・・埋込後処理部
560・・・JPEG'／BMP変換部
562・・・BMP／JPEG'変換部
564・・・DCT係数調整部
502・・・出力フォーマット変換部
60・・・検出部
600・・・検出前処理部
602・・・埋込データ抽出部
604・・・埋込データ計算部
606・・・改ざん検出場所特定部
608・・・出力フォーマット変換部
80・・・OS

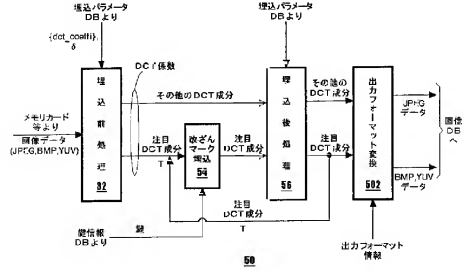
【図16】



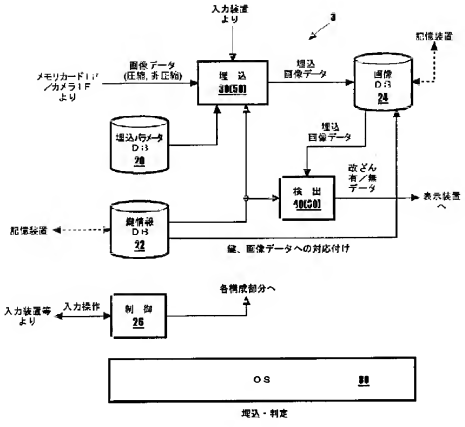
【図1】


100
表示装置
PC本体
110
キーボード
入力装置
102
マウス
メモリ
112
通信装置
118
ディジタル・カメラ
140
104
カメラ
I F
CPU
114
メモリ
カード
メモリ
カード
I F
142
106
記憶装置
108
1
記憶媒体
(CDR,MO等)
170

【図13】

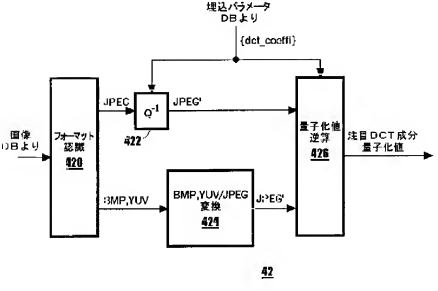

埋込パラメータ
DBより
{dct_coeff(i),
δ
DC/係数
その他のDCT成分
メモリカード
等より
画像データ
(JPEG,BMP,YUV)
埋込前処理
82
注目
DCT成分
T
改ざん
マーク
埋込
84
注目
DCT成分
T
埋込パラメータ
DBより
埋込後処理
86
その他の
DCT成分
注目
DCT成分
出力フォーマット変換
502
JPEG
データ
BMP,YUV
データ
画像
DBへ
注目
DCT成分
T
鍵
鍵情報
DBより
出力フォーマット
情報
50

【図2】


入力装置より
2
記憶装置
メモリカードI/F
カメラI/F
より
画像データ
(圧縮, 非圧縮)
埋込
30(50)
埋込画像データ
画像
D/B
24
埋込パラメータ
D/B
28
埋込
画像データ
改ざん
有/無
データ
検出
40(50)
表示装置
へ
画像情報
D/B
22
鍵、画像データへの対応付け
各構成部分へ
入力装置等
より
入力操作
制御
26
OS
80
埋込・判定

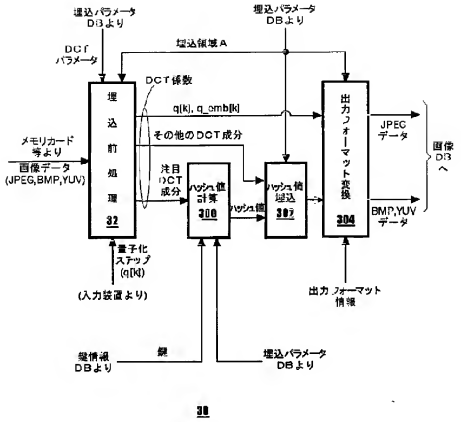
2

【図8】

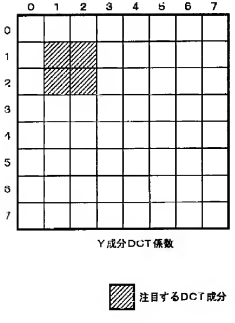

埋込パラメータ
DBより
{dct_coeffi}
JPEG
Q-1
JPEG'
422
画像
DBより
フォーマット
認識
420
量子化値
逆算
426
注目DCT成分
量子化値
BMP,YUV
BMP,YUV/JPEG
変換
424
JPEG'

42

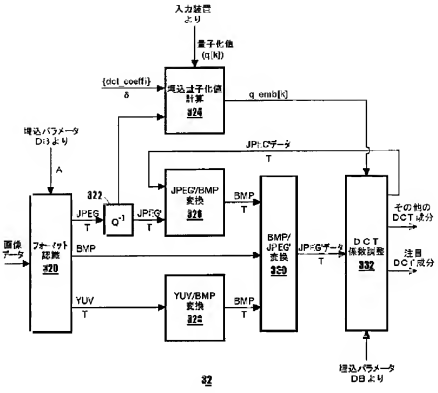
【図3】


埋込パラメータ
DBより
埋込パラメータ
DBより
DCT
パラメータ
埋込領域A
DCT係数
埋込前処理
32
q[k], q_omb[k]
その他のDCT成分
メモリカード
等より
画像データ
(JPEG,BMP,YUV)
注目
DCT
成分
ハッシュ値
計算
300
ハッシュ値
埋込
302
出力フォーマット変換
304
JPEG
データ
BMP,YUV
データ
画像
DB
へ
量子化
ステップ
(q[k])
(入力装置より)
出力フォーマット
情報
鍵情報
DBより
鍵
埋込パラメータ
DBより
30

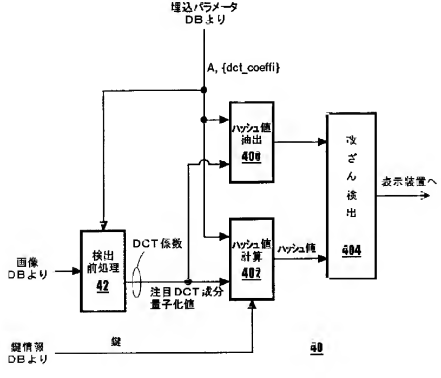
【図4】


0
1
2
3
4
5
6
7
Y成分DCT係数
注目するDCT成分

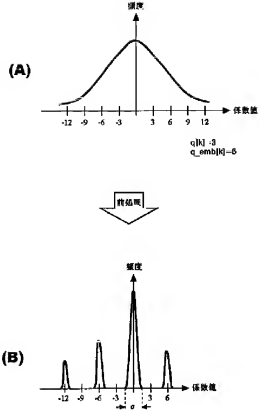
【図5】


入力装置より
量子化値(q(k))
{dct_coeffi}
δ
埋込量子化値計算
324
q_emb[k]
埋込パラメータDBより
A
JPEGデータ
T
322
JPEG
T
Q-1
JPEG
T
JPEG/BMP変換
326
BMP
T
BMP/JPEG変換
328
JPEGデータ
T
DCT係数調整
332
その他のDCT成分
注目DCT成分
画像データ
フォーマット認識
320
BMP
T
YUV
T
YUV/BMP変換
330
BMP
T
埋込パラメータDBより
32

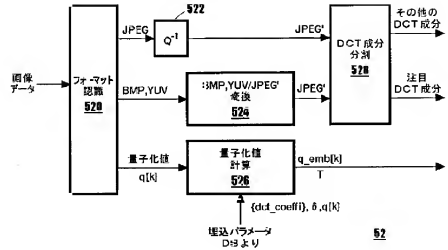
【図7】


埋込パラメータDBより
A, {dct_coeffi}
ハッシュ値抽出
408
改ざん検出
404
表示装置へ
画像DBより
検出前処理
42
DCT係数
注目DCT成分量子化値
ハッシュ値計算
402
ハッシュ値
鍵情報DBより
鍵
40

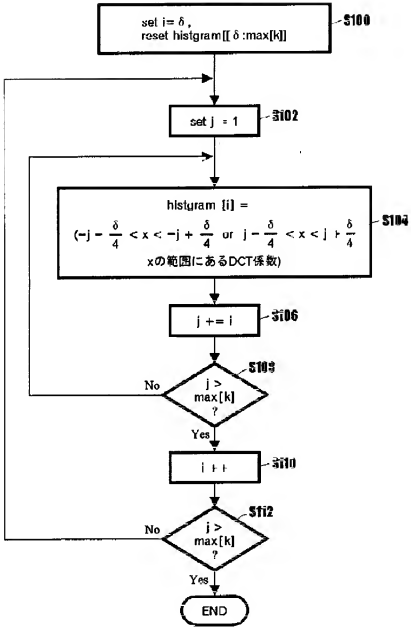
【図６】


(A)
頻度
係数値
-12 -9 -6 -3 3 6 9 12
q[k] -3
q_emb[k]=5
(B)
頻度
係数値
-12 -9 -6 -3 3 6
σ

【図１４】

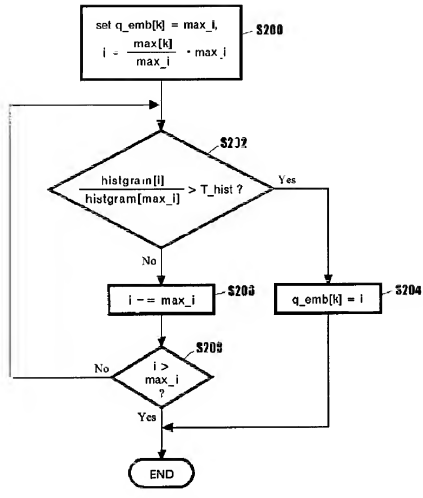

522
JPEG
Q⁻¹
JPEG'
DCT成分分割
528
その他のDCT成分
注目DCT成分
画像データ
フォーマット認識
520
BMP,YUV
:BMP,YUV/JPEG'変換
524
JPEG'
量子化値
q[k]
量子化値計算
526
q_emb[k]
T
{dct_coeff}, δ,q[k]
埋込パラメータD=3より
52

【図9】


set i= δ ,
reset histgram[[δ :max[k]]
S100
set j = 1
S102
histgram [i] =
(−j − δ/4 < x < −j + δ/4 or j − δ/4 < x < j + δ/4
xの範囲にあるDCT係数)
S104
j += i
S106
j > max[k] ?
S108
No
Yes
i + +
S110
j > max[k] ?
S112
No
Yes
END

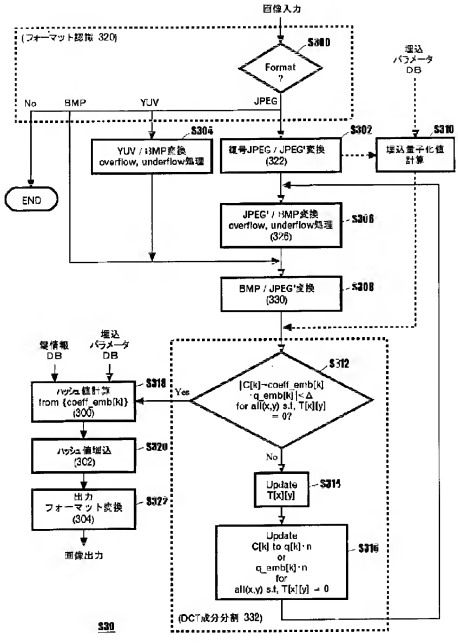
S10

【図10】

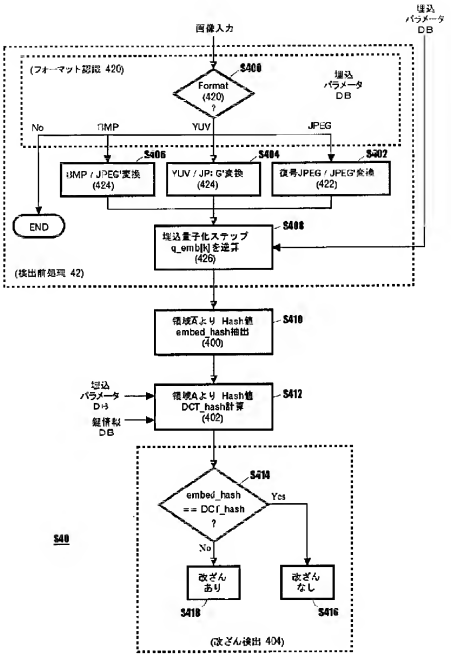

set q_emb[k] = max_i,
i = max[k] / max_i * max_i
S200
S202
histgram[i] / histgram[max_i] > T_hist ?
Yes
No
i -= max_i
S203
q_emb[k] = i
S204
S205
i > max_i ?
No
Yes
END

S20

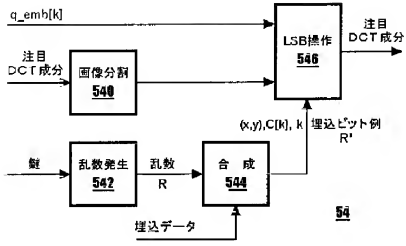
【図11】


画像入力
(フォーマット認識 320)
S300
Format ?
No
BMP
YUV
JPEG
埋込 パラメータ DB
S304
YUV / BMP変換 overflow, underflow処理
S302
復号JPEG / JPEG'変換 (322)
S310
埋込量子化値 計算
END
JPEG' / BMP変換 overflow, underflow処理 (326)
S306
BMP / JPEG'変換 (330)
S308
受情報 DB
埋込 パラメータ DB
S312
|C[k]-coeff_emb[k] -q_emb[k]·n|<Δ for all(x,y) s.t. T[x][y] = 0?
Yes
No
S316
ハッシュ値計算 from {coeff_emb[k]} (300)
S320
ハッシュ値埋込 (302)
S322
出力 フォーマット変換 (304)
画像出力
S314
Update T[x][y]
S318
Update C[k] to q[k]·n or q_emb[k]·n for all(x,y) s.t. T[x][y] = 0
(DCT成分分割 332)
S30

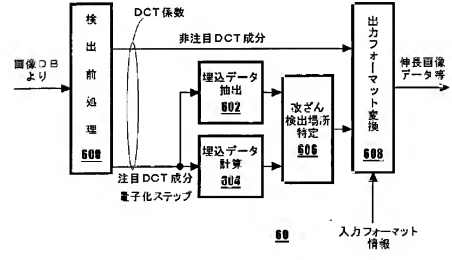
【図12】


埋込
パラメータ
DB
画像入力
(フォーマット認識 420)
S408
Format
(420)
?
埋込
パラメータ
DB
No
BMP
YUV
JPEG
S406
BMP / JPEG'変換
(424)
S404
YUV / JPEG'変換
(424)
S402
復号JPEG / JPEG'変換
(422)
END
S408
埋込量子化ステップ
q_emb[k]を逆算
(426)
(検出前処理 42)
S410
領域Bより Hash値
embed_hash抽出
(400)
埋込
パラメータ
D+3
S412
領域Aより Hash値
DCT_hash計算
(402)
鍵情報
DB
S414
embed_hash
== DCT_hash
?
Yes
No
S40
改ざん
あり
改ざん
なし
S418
S416
(改ざん検出 404)

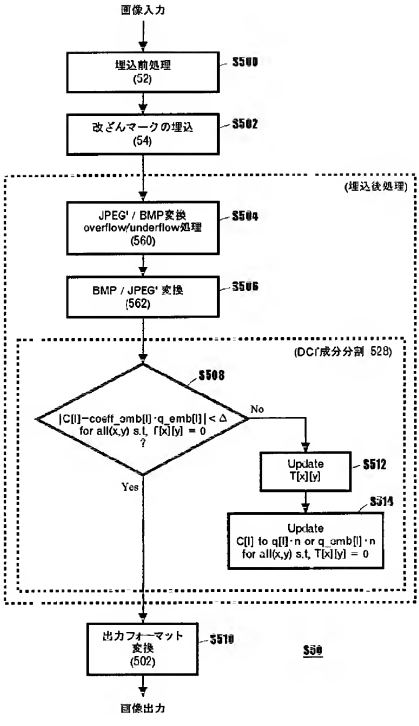
【図15】


q_emb[k]
注目
DCT成分
画像分割
540
LSB操作
546
注目
DCT成分
(x,y),C[k], k
埋込ビット例
R'
鍵
乱数発生
542
乱数
R
合　成
544
54
埋込データ

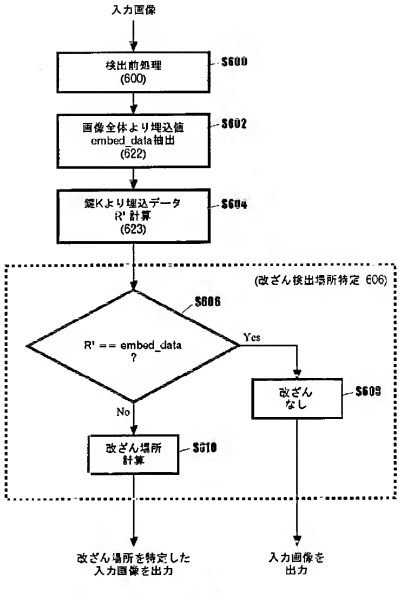
【図17】


検出前処理
600
DCT係数
非注目DCT成分
画像DB
より
埋込データ
抽出
602
埋込データ
計算
604
改ざん
検出場所
特定
606
出力フォーマット変換
608
伸長画像
データ等
注目DCT成分
量子化ステップ
60
入力フォーマット
情報

【図18】


画像入力
埋込前処理
(52)
S500
改ざんマークの埋込
(54)
S502
(埋込後処理)
JPEG' / BMP変換
overflow/underflow処理
(560)
S504
BMP / JPEG' 変換
(562)
S506
(DC/成分分割 528)
S508
|C[i]−coeff_emb[i]·q_emb[i]| < Δ
for all(x,y) s.t. T[x][y] = 0
?
No
Yes
Update
T[x][y]
S512
S514
Update
C[i] to q[i]·n or q_emb[i]·n
for all(x,y) s.t. T[x][y] = 0
出力フォーマット
変換
(502)
S510
S50
画像出力

【図19】



S60

フロントページの続き

(51)Int.Cl.⁷	識別記号	FI	(参考)
H04N 7/30		H04N 7/133	Z 5C078

(72)発明者 上條 浩一
神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内

(72)発明者 森本 典繁
神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内

(72)発明者　利根川　聡子
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

Fターム(参考)　5B057 AA11 CA01 CA08 CA12 CA16 CB01 CB08 CB12 CB16 CB19 CE08 CG05 CG09 CH01 CH11
5C053 FA08 FA13 FA27 GB06 GB07 GB21 GB22 GB26 GB33 GB36 GB40 JA21 JA30 KA05 LA06
5C059 KK35 KK43 LA02 MA00 MA23 MD02 PP01 PP14 RC35 SS15 SS20
5C076 AA14 AA36 AA40 BA06 BA09
5C077 LL14 MP08 NP01 PP21 PP23 PQ12 PQ22 RR21 RR30
5C078 AA09 BA57 CA14 CA17 DA01 DA02